Name Constraints Extension

References: X.509 sections: 12.1, 12.4.2.2, K.2
RFC 2459 sections: 4.1.2.4, 4.2, 4.2.1.7, 4.2.1.11, and 10
FPKI Profile sections: 1.2.12, 3.2.2.1
MISPC sections: 1.4, 3.1.3.3
DII PKI Functional Specification section: 3.2.2.3

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Does the certificate issuer enable the nameConstraints (NC) extension in CA certificates?		
Does the certificate issuer not include the NC extension in a self-signed certificate?		
Does the certificate issuer not include the NC extension in an EE certificate?		
Does the certificate issuer flag the NC extension critical when it is present?		
Does the certificate issuer only use name forms that have a standard-defined hierarchical structure in the NC extension?		
Can the certificate issuer use either permittedSubtrees or excludedSubtrees to establish restrictions?		
Is permittedSubtrees the preferred choice?		
Does the certificate issuer always fill the NC base component?		
Does the certificate issuer set the NC base component to a CA at the root of a subtree?		
Does the certificate issuer set 0 as the default value of the minimum component?		
Does the certificate issuer leave the maximum component absent as		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
When the certificate issuer establishes restrictions for IPv4 addresses, does the ipAddress field of generalName contain eight (8) octets, encoded in the style of RFC 1519 (CIDR) to represent an address range?		
When the certificate issuer establishes restrictions for IPv6 addresses, does the ipAddress field of generalName contain 32 octets, encoded in the style of RFC 1519 (CIDR) to represent an address range?		
Does the application processing the certificate recognize the NC extension?		
In processing a received certificate with the NC extension present, does the certificate user recognize it as a CA certificate?		
If permittedSubtrees is present, does the certificate user validate only those certificates issued by CAs from restricted name space?		
If excludedSubtrees is present, does the certificate user invalidate only those certificates issued by CAs from restricted name space?		
If both permittedSubtrees and excludedSubtrees are present and the name space overlaps, does the certificate user invalidate certificates issued by CAs from the overlapping name space?		
Is a received critical certificate considered invalid if the certificate user does not recognize the name form used in the base component?		
If a non-critical certificate with an unrecognized name form in the base component is received, does the certificate user ignore the name space restriction.		
If the certificate carries multiple names in an acceptable name form, does the certificate user test each of the names against the restricted name space?		
If the certificate's subject name(s) is not in the name form specified in the base component, does the certificate user accept the certificate?		
Does the certificate user test the contents in non-critical subjectAltName extension against the restricted name space?		
If the minimum component is set to 0, does the certificate user include the subtree root designated in the base component in the restricted name space?		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
If the maximum component is more than 0, does the certificate user limit the subtree's name space to the n^{th} subordinate node?		
If the maximum component is present, does the certificate user exclude from the name space all subtree nodes below the set lower limit?		
If the name form is an URI domain (begins with a period (.xyz.com)), does the certificate user apply the constraint to one or more subdomains?		
If the name form is an URI domain (begins with a period (.xyz.com)), does the certificate user not apply the constraint to the host (xyz.com)?		
If the name form is an URI host (does not begin with a period (xyz.com)), does the certificate user apply the constraint to the host?		
If the name form is an Internet mail address, does the certificate user interpret a complete mail address as a restriction to that mailbox only?		
If the name form is an Internet mail address, does the certificate user interpret a host name as a restriction to all mailboxes on that host?		
If the name form is an Internet mail address, does the certificate user interpret a domain name (.xyz.com) as a restriction to any address in that domain?		
If the name form is a DNS name (pki.xyz.com), does the certificate user apply the constraint to any subdomain?		
The name form in the certificate is an RFC 822 name embedded in the subject distinguished name (DN) in an attribute of type EmailAddress, and there is no subjectAltName extension. Does the certificate user apply the constraint to the attribute of type EmailAddress in the subject DN?		
If the directoryName name form is used, does the certificate user apply the constraint to the subject field, and the directoryName types in the subjectAltName extension?		
When applying restrictions of the form directoryName, does the certificate user consider DN attributes?		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
When applying restrictions of the form directoryName, does the certificate user perform the following DN comparison rules: (a) attribute values encoded in different types represent different strings; (b) attribute values in types other than PrintableString are case sensitive; (c) attribute values in PrintableString are not case sensitive; and (d) attribute values in PrintableString are compared after removing leading and trailing white space and converting internal substrings of one or more consecutive white space characters to a single space?		
If the x400Address name form is used, does the certificate user apply the constraint to x400Address types in the subjectAltName extension?		
If the iPAddress name form is used, does the certificate user apply the constraint to iPAddress types in the subjectAltName extension?		
If a self-signed certificate has a non-critical NC extension, does the certificate user accept the certificate but not apply the restriction?		
If a self-signed certificate has a critical NC extension, does the certificate user invalidate the certificate?		

Other information:

In processing a received certificate, if the certificate fails validation what does the implementation do?

None of processing cases is prohibited by the standards, so implementations should be capable of receiving and processing them. Issuing CA certificates is mandatory for implementations.

Recommendations for Standards Work: